WHAT IS CLAIMED IS:

1. A method of presenting data related to an intrusion event on a computer system, comprising:

capturing data related to the intrusion event;

decoding the captured data from a predetermined format to a predetermined format decipherable by humans, the decoded data in turn comprises intrusion event data, data summary, and detailed data; and

presenting the decoded data to a user in an organized manner.

2. The method, as set forth in claim 1, wherein capturing data comprises capturing network data packets of the intrusion event.

3. The method, as set forth in claim 1, wherein decoding the captured data comprises decoding the captured data from a binary format to a human-readable text format.

4. The method, as set forth in claim 1, wherein decoding the captured data comprises decoding the captured data to decoded data having a data link layer protocol header, a network layer protocol header, a network layer protocol data summary, and packet data in hexadecimal format.

5. The method, as set forth in claim 1, wherein decoding the captured data comprises decoding the captured data to decoded data having an Ethernet header, an IP header, an IP data summary, and packet data in hexadecimal format.

6. The method, as set forth in claim 1, wherein presenting the decoded data comprises displaying the decoded data on a computer screen.

7. The method, as set forth in claim 1, wherein presenting the decoded data comprises graphically displaying the decoded data according to a predetermined report organization and format.

8. The method, as set forth in claim 1, wherein presenting the decoded data comprises generating a report having the decoded data.

9. A method of presenting data of an intrusion detection system, comprising:

capturing, from a network, data related to an intrusion event in response to a trigger;

decoding the captured data from a first predetermined format to a second predetermined format, the decoded data comprising network header data, data summary, and detailed data; and

presenting the decoded data according to a predetermined report format.

10. The method, as set forth in claim 9, wherein capturing data comprises capturing network data packets of the intrusion event in response to detecting the presence of a predetermined signature in the network data packet.

11. The method, as set forth in claim 9, wherein decoding the captured data comprises decoding the captured data from a binary format to a human-readable text format.

12. The method, as set forth in claim 9, wherein decoding the captured data comprises decoding the captured data to decoded data having a data link layer protocol header, a network layer protocol header, a network layer protocol data summary, and packet data in hexadecimal format.

13. The method, as set forth in claim 9, wherein decoding the captured data comprises decoding the captured data to decoded data having an Ethernet header, an IP header, an IP data summary, and packet data in hexadecimal format.

14. The method, as set forth in claim 9, wherein presenting the decoded data comprises graphically displaying the decoded data according to a predetermined report format and organization.

15. The method, as set forth in claim 1, wherein presenting the decoded data comprises generating a report having the decoded data.

16. A system of presenting data of an intrusion detection system, comprising:

a network driver capturing data related to an intrusion event from a network;

a decode engine decoding the captured data from a predetermined format to a predetermined format decipherable by humans, the decoded data comprising intrusion event data, data summary, and detailed data; and

a user interface presenting the decoded data to a user.

17. The system, as set forth in claim 16, wherein the network driver captures network data packets of the intrusion event in response to the intrusion detection system detecting a predetermined intrusion signature.

18. The system, as set forth in claim 16, wherein the decode engine decodes the captured data from a binary format to a human-readable text format.

19. The system, as set forth in claim 16, wherein the decode engine decodes the captured data to decoded data having a data link layer protocol header, a network layer protocol header, a network layer protocol data summary, and packet data in hexadecimal format.

20. The system, as set forth in claim 16, wherein the decode engine decodes the captured data to decoded data having an Ethernet header, an IP header, an IP data summary, and packet data in hexadecimal format.

21. The system, as set forth in claim 16, wherein the user interface displays the decoded data on a computer screen.

22. The system, as set forth in claim 16, wherein the user interface graphically displaying the decoded data according to a predetermined report organization and format.

23. The system, as set forth in claim 16, wherein the user interface generates a report having the decoded data.